DRAFT - April 19, 1999

INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy" standard on personal data transfers from the European Community to the United States. Personal data is data about an identified or identifiable individual that is recorded in any form.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing these principles under its statutory authority to foster, promote, and develop international commerce. The principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because these principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate.

Organizations may qualify for the safe harbor in different ways. If an organization joins a private sector developed privacy program that adheres to these principles, it qualifies for the safe harbor.

Where an organization is subject to US statutory, regulatory, administrative or other body of law (or body of rules issued by national

securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that also effectively protects personal data privacy, it qualifies for the safe harbor to the extent that its activities are governed by such laws or rules. Organizations may also put in place the safeguards deemed necessary by the EU for transfers of personal data from the EU to the US by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the EU.(1)*

*Numbers in parentheses (1-7) refer to endnotes.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, but organizations that decide to adhere to these principles must comply with these principles in order to obtain and retain the benefits of the safe harbor as described in _____ and publicly declare that they do so. All organizations qualifying for the safe harbor should for purposes of transparency and other beneficial reasons notify the Department of Commerce or its nominee in accordance with the guidance set forth in _____.

In addition to any exceptions provided for by the Directive and EU Member State law,(2) adherence to these principles may be limited to the extent necessary to meet US national security, public interest, and law enforcement requirements as well as other US statutory and regulatory provisions. Adherence to these principles is not required for participation in the safe harbor where data is manually processed.(3)

Safe Harbor Principles

1. NOTICE: An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally

collected or discloses it to a third party.

2. CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.(4)

3. ONWARD TRANSFER: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.(5)

4. SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. DATA INTEGRITY: Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current.

6. ACCESS: Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct

or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.](6)

7. ENFORCEMENT: Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which an individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

*Note: Mechanisms for assuring compliance with the safe harbor principles may take different forms. Organizations may satisfy the requirements set forth in Principle 7 through the following mechanisms: (1) through compliance with private sector developed privacy programs that include effective enforcement mechanisms of the type described in Principle 7; (2) through compliance with legal or regulatory supervisory authorities; or (3) by committing to cooperate with data protection authorities located in the European Community or their authorized representatives, provided those authorities agree. This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of these principles.***(7)**

Endnotes

1. **The Commission has not agreed to this sentence and will raise this issue with the Member States.**
2. **The Commission does not consider it appropriate to refer directly to the provisions of the Directive or to EU Member State law.**

3. This text is not agreed by the Commission on the grounds that only certain requirements of the Directive are deferred for manually processed data.
4. The US notes that explicit (opt in) choice is not necessarily required under the Directive for sensitive information where the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care or diagnosis and will cover this in a Frequently Asked Question (FAQ).
5. The Commission would like text added to the Onward Transfer principle that requires explicit notice and choice when personal data is transferred to a third party that does not adhere to the safe harbor requirements.
6. The Commission proposes to delete the words in square brackets, but could accept alternative wording to show that the right to access is not absolute. Specific obligations under the access principle are spelled out in the FAQs.
7. The Commission would prefer to see this text as a continuation of principle 7. The EC would also like the text to state clearly that all the requirements of principle 7 must be met for all participants in the safe harbor. The EC is consulting its data protection authorities about point (3) in the note.